Notes (02/19/2024)

Classification of Cyber Crimes

What is a Crime: An act or the commission of an act that is forbidden, or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment by that law.

- **Cybercrime against individual**
    - **Electronic mail spoofing and other online frauds:**
        - A spoofed EMail is one that appears to originate from one source but actually has been sent from another source.
        - For example let us say stanley has an EMail address stanley@asianlaws.org. Let us say his friend Stella and him happen to have a showdown. Then Stella, having become his enemy, spoofs her EMail and sends vulgar messages to all her acquaintances. Since the E-Mails appear to have originated from stanley his friends could take offense and spoil relationships among themselves.
    - **Phishing, spear phishing and its various other forms such as vishing & smishing:**
        - **Phishing**—It is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.
        - **Spear phishing**—It is a targeted cyberattack toward an individual or organization with the end goal of receiving confidential information for fraudulent purposes.
        - **How phishing works**—Threat actor identifies a target > Sends legitimate-looking email > Victim opens the email containing malware > Hacker gains access to steal data.
        - **Vishing**—Criminal practice of using social engineering over the telephone system, most often using features facilitated by VoIP, to gain access to personal and financial information from the public for the purpose of financial reward. The term is a combination of V-voice phishing. Vishing is used to steal credit card numbers or other related data used in ID theft schemes from individuals.
        - **Smishing**—It is a criminal offense conducted by using social engineering techniques similar to phishing. The name is derived from “SMS phishing”. Smishing uses cell phones text messages & It works

similarly like vishing. Examples: "we are happy to send our confirmation toward your enrollment for our YourNameHereClub membership, you will be charged Rs 50 per day unless you reconfirm your acceptance of your membership on your Membership office contact number XXXXXXXXX.".

- **Spamming:**
  - People who create electronic spam are called spammers.
  - Spam is abuse of electronic messaging systems to send bulk messages indiscriminately.
  - Most widely recognised form of spam is EMail spam.
  - Spamming is difficult to control because it has economic viability.
- **Cyber defamation:**
  - **DEFAMATION**—defamation is where a person intentionally spreads information about another person by which that person loses reputation. Cyber Defamation is not a specific cyber offense though the internet is being used to spread fake news.
  - **CYBER DEFAMATION**—And defamation on the internet just like the other types of defamation likewise cyber defamation is against the law.
  - An example of cyber defamation is when someone sends an email saying hurtful things about you to someone else or posting false things about you on the internet.
- **Cyberstalking and harassment:**
  - Stalking basically means trying to approach somebody or something.
  - Cyberstalking has been defined as use of information and communication technology, particularly the internet by an individual or group of individuals to harass another individual or group of individuals.
  - Two types of stalkers are online stalkers and offline stalkers. The majority of cyber stalkers are men and the victims are women. It happens between people who have prior relationships but also there are many instances of strangers.
- **Computer sabotage:**
  - It's the process of alteration or suppression of computer data or programmes with the intention of hindering the functioning of computers.
  - It is performed through worms, logic bombs and virus
  - **Example:** Y2k bug: actually called the year 2000 bug or the millennium bug is a problem in the coding of computerized systems that was projected to create computer networks around the world.

    - **Por***raphic offenses:**
        - Child por***raphy is considered an offense. Unfortunately it's the reality of the internet. The internet is being highly used by the abusers to reach and abuse children worldwide.
        - COPPA: children's online privacy protection act is a way of preventing online por***raphy.
    - **Password sniffing:**
        - SNIFFING: technique for gaining access through network based attack.
        - The most important thing typically to sniff is authentication information, the examples of authentication information is usernames and passwords.
- **<u>Cybercrime against property</u>**
    - **Credit card frauds:**
        - At its simplest, credit card fraud can involve stealing someone's physical credit or debit card and using it to make purchases. However, that type of credit card fraud is becoming rarer by the day. In fact, after the introduction of Europay, Mastercard, and Visa (EMV) chips, card present fraud at the point of sale significantly declined, while card-not-present (CNP) fraud drastically increased.
        - **How to avoid:** 1) Keep your credit cards safe. Store your cards in a secure wallet or purse. After making a purchase. immediately return your card to that place. 2) Don't allow websites to "remember" your card number. Only let secure payment portals, like GooglePay and PayPal, remember your card number. An even better practice is to never check the "remember card number" box for any site or portal. 3) Be wary when shopping online. Before using your credit card online, verify the site's security and that the URL is authentic—there's an "s" after the "http" in the web address, and a lock icon as well. 4) Report lost or stolen cards immediately. The sooner you report a missing card, the less liability you'll have for fraudulent charges made with your card. 5) Review your monthly bill. Always look through your monthly statement to check for suspicious account activity.
    - **Intellectual property crimes:**
        - Intellectual property crime is committed when someone manufactures, sells or distributes counterfeit or pirated goods, such as such as patents, trademarks, industrial designs or literary and artistic works, for commercial gain.
        - The four kinds of intellectual property are patents, trademarks, copyrights and trade secrets.

- **Internet time theft:**
  - One of the most common forms of time theft, this is when employees use the internet for non-work purposes. They could be using it for browsing the internet, online shopping, playing games, or spending bulks of time on social media.

- **<u>Cybercrime against organization</u>**
  - **Unauthorized accessing of computer:**
    - Every act committed towards breaking into a computer and/or network is hacking, and hacking is one of the methods of accessing computers without approval.
  - **Denial-of-service attacks:**
    - Attack meant to shut down a system or network, making it inaccessible to its intended users.
    - DOS attackers accomplish this by flooding the target with traffic or by sending it information that triggers a crash.
    - DOS attack deprives legitimate users i.e, members, of the service or resources they expected.
    - Ex: websites, email, banking domain, etc.
  - **Virus attack/dissemination of viruses:**
    - Computer virus is a program that can infect legitimate programs by modifying them to include a possibly evolved copy of itself.
    - Viruses may also contain malicious instructions that may cause damage.
    - The combination of possibly malicious code with the ability to spread is what makes it a considerable concern.
  - **E-mail bombing/Mail bombs:**
    - Sending a large number of emails to the victim to crash victims email account or to make victims email server crash.
    - By instructing a computer to repeatedly send email to specified persons email address the cybercriminal can overwhelm the recipient's personal account and potentially shut down the entire system.
  - **Salami attack/salami technique:**
    - The attackers are used for committing financial crimes. Bank employee inserts a program into the bank's servers that deducts a small amount of money from the account of every customer.
    - No account holder will probably notice this unauthorized debit but the bank employee will make a sizable amount every month.
  - **Logic bomb:**

        - Event dependent programs created to do something only when a certain event occurred (known as trigger event).
        - Some viruses can also be termed as logic bombs because they lie dormant all through the years and become active only on a particular date.
        - Ex: carbonyl virus attack and 2k virus.
    - **Trojan horse:**
        - Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programing has data in a way that it can get control and cause harm, for example ruining the file allocation on the hard disk.
    - **Data diddling:**
        - Involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.
        - Electricity boards in India have been victims to data diddling programs inserted when private parties computerize their systems.
    - **Software piracy:**
        - It is an act of stealing a software that is legally protected.
        - Stealing includes copying, distributing, modifying, or selling software.
- **<u>Cybercrime against society</u>**
    - **Cyberterrorism:**
        - Cyberterrorism is the use of the internet to conduct violent acts that result in, or threaten, the loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation. Acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet by means of tools such as computer viruses, phishing, malicious software, hardware methods, programming scripts can all be forms of internet terrorism.
    - **Forgery:**
        - Currency notes, postage and revenue stamps, marksheets, etc. can be forged using sophisticated computers, printers and scanners. Outside many colleges there are miscreants soliciting the sale of fake marksheets or even degree certificates. These are made using computers and high quality scanners and printers. In fact, this is becoming a booming business involving large monetary amounts given to student gangs in exchange for these bogus but authentic looking certificates.
    - **Web Jacking:**

        - Web jacking occurs when someone forcefully takes control of a website (by cracking the password and later changing it). Thus, the first stage of this crime involves "password sniffing." The actual owner of the website does not have any more control over what appears on that website.
- **Crimes emanating from user network newsgroup**
    - **Description:**
        - A Usenet newsgroup is a repository usually within the Usenet system, for messages posted from users in different locations using the Internet. They are discussion groups and are not devoted to publishing news.
- **Safety checklist:**
    - **1)** Back up online and offline files regularly and securely.
    - **2)** Strengthen your home network.
    - **3)** Use strong passwords.
    - **4)** Keep your software updated.
    - **5)** Manage social media pages.
    - **6)** Check privacy and security settings.
    - **7)** Avoid opening and deleting suspicious emails or attachments.

Also view at: https://sites.google.com/view/owca/notes/02-19-2024